Remarks

Reconsideration of this Application is respectfully requested.

Upon entry of the foregoing amendment, claims 1-9 and 12-19 are pending in the application, with claims 1 and 12 being the independent claims. Claims 1 and 12 are sought to be amended. These changes are believed to introduce no new matter, and their entry is respectfully requested.

Based on the above amendment and the following remarks, Applicants respectfully request that the Examiner reconsider all outstanding objections and rejections and that they be withdrawn.

Rejections under 35 U.S.C. § 103

Claims 1-9 and 12-19 were rejected under 35 U.S.C. §103(a) as being unpatentable over Ziai, U.S. Patent No. 7,017,042 (Ziai) in view of Anand, U.S. Patent No. 7,266,703 (Anand). Applicants respectfully traverse this rejection.

The combination of Ziai and Anand do not teach or suggest each and every limitation of Applicant's amended independent claims 1 and 12. Ziai describes a network protocol offload chip 400 having an IPSec decryption accelerator 402 and the IPSec encryption accelerator 411. (Ziai, FIG. 4). As IP packets are received by the network protocol offload chip's 400 inbound network interface 401, network interface logic 450 forwards the received packets to the IPSec decryption accelerator 402. (Ziai, col. 7, lines 25-30). "While the packets are waiting to be analyzed by the IPSec decryption accelerator 402, they will be placed in the inbound packet buffer 403." (Ziai, col. 7, lines 30-34).

Further, in Ziai, system interface 407 receives application data sent by system CPU 408. (Ziai, col. 9, lines 1-3). After TCP/IP processing, IP packets enter buffer 418. Next, IPSec encryption accelerator 411 performs IPSec processing on the IP Packets from buffer 418 requiring IPSec processing. (Ziai, col. 9, lines 18-45). As described in Ziai, IPSec encryption accelerator 411 has an input buffer 418 and IPSec decryption accelerator 403 has a separate input buffer 403. IPSec encryption accelerator 411 does not share an input buffer with IPSec decryption accelerator 403.

Anand does not overcome these deficiencies of Ziai. FIG. 2 of Anand "illustrates the architecture of cryptographic processor 112 for a single independent channel of cryptographic core 112. The other three independent channels (not shown) may be handled in a similar manner." (Anand, para. [0030]). Thus, only the blocks for a single channel are shown in FIG. 2, except that cipher block 204 handles all four channels. (Anand, FIG. 2). As shown in FIG. 2 of Anand, each channel includes an input FIFO 208 and an output FIFO 210. The four channels associated with cipher block 204 therefore do not share an input buffer. Furthermore, the cipher block 204 is coupled to four input FIFOs, one per each channel.

Accordingly, the combination of Ziai and Anand does not teach or suggest "a plurality of cryptographic processing cores, each cryptographic processing core having a plurality of data paths, and an input buffer shared among the plurality of input ports and the plurality of data paths associated with each cryptographic processing core in the plurality of cryptographic processing cores," as recited in amended independent claims 1 and 12.

Furthermore, Ziai describes that Direct Memory Access (DMA) is used to send the IP packet to Network Offload Memory (NOM) 405:

> After IPSec processing 303b at the acceleration device 302, the IP packet is sent (e.g., via a Direct Memory Access (DMA)) 304b to the Network Offload Memory (NOM) 304. Information is transferred directly to and from memory by many devices over DMA channels. A DMA channel is a system pathway. DMA is a method to transfer large quantities of data, or to make high-speed transfers of data in which individual transfer cycles are not the responsibility of the system CPU. A separate DMA controller unit 404 may be used to manage each data transfer.

(Ziai, col. 4, lines 36-45). Nowhere does Ziai teach or suggest that DMA is used by the IPSec Encryption or Decryption Accelerators to access the security association database (SAD) or the security policy database (SPD).

Instead, in Ziai, the SPD 308 and SAD 309 "may be contained in one database or two databases. Furthermore, in alternate embodiments, the SPD 308 and SAD 309 may be contained within a memory chip or within multiple memory chips. In still further embodiments, the SPD 308 and SAD 309 may be maintained within a register or within multiple registers." (Ziai, col. 6, lines 26-32). Thus, Ziai describes the SPD and SAD as onchip memory. *See* FIG. 4 of Ziai. Applicants' recited amendment overcomes the limitations of accessing security association information from system memory or onchip memory, such as described in Ziai. As discussed in Applicants' specification:

> Because time taken to access bus controller memory is substantially greater than the time taken to access other forms of memory, security association information is typically held in random access memory or in onchip memory. Nonetheless, the techniques of the present invention recognize that there are benefits to allowing the retrieval of security association information from bus controller memory 823.

(Publication of Applicants' Specification, US2004/0123123, ¶0060).

Thus, the combination of Ziai and Anand also does not teach or suggest "a security association lookup unit configured to identify a security association address in a first portion of an address space associated with the cryptography accelerator by using header information, the first portion of the address space corresponding to bus controller memory, wherein the security association lookup unit is operable to acquire the security association information from bus controller memory," as recited in amended independent claim 1 or "a policy security association lookup unit configured to issue a read request to a bus controller memory for security association information for a first data packet and to process a second data packet prior to receipt of the read response for the first data packet, wherein the bus controller memory is separate from a system memory," as recited in amended independent claim 12.

For at least these reasons, amended independent claims 1 and 12 are patentable over the combination of Ziai and Anand. Claims 2-9 depend from claim 1 and claims 13-19 depend from claim 12. For at least these reasons, and further in view of their own features, claims 2-9 and 13-19 are also patentable over the combination of Ziai and Anand. Reconsideration and withdrawal of the rejection are therefore respectfully requested

Conclusion

All of the stated grounds of objection and rejection have been properly traversed, accommodated, or rendered moot. Applicants therefore respectfully request that the Examiner reconsider all presently outstanding objections and

rejections and that they be withdrawn. Applicants believe that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Amendment and Reply is respectfully requested.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

Lori A. Gordon
Attorney for Applicants
Registration No. 50,633

Date: April 16, 2008

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600
772953_1.DOC